

N10-008 Dumps

CompTIA Network+Exam

<https://www.certleader.com/N10-008-dumps.html>



NEW QUESTION 1

- (Topic 1)

A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter. Which of the following ports should be blocked when checking firewall configuration?

- A. 22
- B. 23
- C. 80
- D. 3389
- E. 8080

Answer: B

Explanation:

Port 23 should be blocked when checking firewall configuration to prevent outside users from telnetting into any of the servers at the datacenter. Port 23 is the default port for Telnet, which is an insecure protocol that allows remote access to servers and network devices. Telnet sends data in clear text, which can be easily intercepted and compromised by attackers. A more secure alternative is SSH, which uses port 22 and encrypts data. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 2

- (Topic 1)

A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds that jitter at the office is greater than 10ms on the only WAN connection available. Which of the following would be MOST affected by this statistic?

- A. A VoIP sales call with a customer
- B. An in-office video call with a coworker
- C. Routing table from the ISP
- D. Firewall CPU processing time

Answer: A

Explanation:

A VoIP sales call with a customer would be most affected by jitter greater than 10ms on the WAN connection. Jitter is the variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms. References: <https://www.voip-info.org/voip-jitter/>

NEW QUESTION 3

- (Topic 1)

Which of the following DNS records works as an alias to another record?

- A. AAAA
- B. CNAME
- C. MX
- D. SOA

Answer: B

Explanation:

The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.

References:

? CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.

NEW QUESTION 4

- (Topic 1)

A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

- A. MIMO
- B. TKIP
- C. LTE
- D. SSID

Answer: D

Explanation:

SSID (Service Set Identifier) is a feature that should be configured to allow different wireless access through the same equipment. SSID is the name of a wireless network that identifies it from other networks in the same area. A wireless access point (AP) can support multiple SSIDs with different security settings and network policies. For example, a store owner can create one SSID for business equipment and another SSID for patron use, and assign different passwords, VLANs, and QoS levels for each SSID. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70931-multiple-ssid.html>

NEW QUESTION 5

- (Topic 1)

A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- A. CDMA
- B. CSMA/CD
- C. CSMA/CA
- D. GSM

Answer: C

Explanation:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

NEW QUESTION 6

- (Topic 1)

A company built a new building at its headquarters location. The new building is connected to the company's LAN via fiber-optic cable. Multiple users in the new building are unable to access the company's intranet site via their web browser, but they are able to access internet sites. Which of the following describes how the network administrator can resolve this issue?

- A. Correct the DNS server entries in the DHCP scope
- B. Correct the external firewall gateway address
- C. Correct the NTP server settings on the clients
- D. Correct a TFTP Issue on the company's server

Answer: A

Explanation:

If multiple users in a new building are unable to access the company's intranet site via their web browser but are able to access internet sites, the network administrator can resolve this issue by correcting the DNS server entries in the DHCP scope. The DHCP scope is responsible for assigning IP addresses and DNS server addresses to clients. If the DNS server entries are incorrect, clients will not be able to access intranet sites.

References:

? CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

NEW QUESTION 7

- (Topic 1)

An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

- A. Pass-the-hash attack
- B. Rainbow table attack
- C. Brute-force attack
- D. Dictionary attack

Answer: D

Explanation:

The attacker attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt is using a dictionary attack. References: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

NEW QUESTION 8

- (Topic 1)

Which of the following technologies provides a failover mechanism for the default gateway?

- A. FHRP
- B. LACP
- C. OSPF
- D. STP

Answer: A

Explanation:

First Hop Redundancy Protocol (FHRP) provides a failover mechanism for the default gateway, allowing a backup gateway to take over if the primary gateway fails. References: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

NEW QUESTION 9

- (Topic 1)

A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

Software on the workstation needs to send a query to the local subnet broadcast address. To which of the following addresses should the software be configured to send the query?

- A. 10.1.2.0
- B. 10.1.2.1

- C. 10.1.2.23
- D. 10.1.2.255
- E. 10.1.2.31

Answer: D

Explanation:

The software on the workstation should be configured to send the query to 10.1.2.255, which is the local subnet broadcast address. A broadcast address is a special address that allows a device to send a message to all devices on the same subnet. It is usually derived by setting all the host bits to 1 in the network address. In this case, the network address is 10.1.2.0/27, which has 27 network bits and 5 host bits. By setting all the host bits to 1, we get 10.1.2.31 as the broadcast address in decimal notation, or 10.1.2.255 in dotted decimal notation. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 10

- (Topic 1)

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:
Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down
Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down
Which of the following describes the reason why the events are not being received?

- A. The network device is not configured to log that level to the syslog server
- B. The network device was down and could not send the event
- C. The syslog server is not compatible with the network device
- D. The syslog server did not have the correct MIB loaded to receive the message

Answer: A

Explanation:

The reason why the alerts are not being received is that the network device is not configured to log that level to the syslog server. The severity level for the events may need to be adjusted in order for them to be sent to the syslog server. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

NEW QUESTION 10

- (Topic 1)

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

- A. SSO
- B. TACACS+
- C. Zero Trust
- D. Separation of duties
- E. Multifactor authentication

Answer: B

Explanation:

TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.

References:

? Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

NEW QUESTION 15

- (Topic 1)

Which of the following is used to track and document various types of known vulnerabilities?

- A. CVE
- B. Penetration testing
- C. Zero-day
- D. SIEM
- E. Least privilege

Answer: A

Explanation:

CVE stands for Common Vulnerabilities and Exposures, which is a list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services. CVE provides a standardized identifier and description for each vulnerability, as well as references to related sources of information. CVE helps to track and document various types of known vulnerabilities and facilitates communication and coordination among security professionals. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://cve.mitre.org/cve/>

NEW QUESTION 20

- (Topic 1)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- A. OSPF
- B. BGP
- C. EGRIP
- D. RIP

Answer: B

Explanation:

BGP (Border Gateway Protocol) is a routing protocol used to exchange route information between public autonomous systems (AS). OSPF (Open Shortest Path First), EGRIP (Enhanced Interior Gateway Routing Protocol), and RIP (Routing Information Protocol) are all used for internal routing within a single AS. Therefore, BGP is the correct option to choose for this question.

References:

? Network+ N10-007 Certification Exam Objectives, Objective 3.3: Given a scenario, configure and apply the appropriate routing protocol.

? Cisco: Border Gateway Protocol (BGP) Overview

NEW QUESTION 23

- (Topic 1)

A user tries to ping 192.168.1.100 from the command prompt on the 192.168.2.101 network but gets the following response: U.U.U.U. Which of the following needs to be configured for these networks to reach each other?

- A. Network address translation
- B. Default gateway
- C. Loopback
- D. Routing protocol

Answer: B

Explanation:

A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device.

References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.techopedia.com/definition/25761/default-gateway>

NEW QUESTION 25

- (Topic 1)

Within the realm of network security, Zero Trust:

- A. prevents attackers from moving laterally through a system.
- B. allows a server to communicate with outside networks without a firewall.
- C. block malicious software that is too new to be found in virus definitions.
- D. stops infected files from being downloaded via websites.

Answer: A

Explanation:

Zero Trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust prevents attackers from moving laterally through a system by applying granular policies and controls based on the principle of least privilege and by segmenting and encrypting data flows across the network. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>

NEW QUESTION 28

- (Topic 1)

A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day. Which of the following is the MOST likely cause of this issue?

- A. The AP association time is set too low
- B. EIRP needs to be boosted
- C. Channel overlap is occurring
- D. The RSSI is misreported

Answer: C

Explanation:

Channel overlap is a common cause of wireless connectivity issues, especially in high-density environments where multiple APs are operating on the same or adjacent frequencies. Channel overlap can cause interference, signal degradation, and performance loss for wireless devices. The AP association time, EIRP, and RSSI are not likely to cause frequent disconnects and reconnects for wireless users.

NEW QUESTION 32

- (Topic 1)

Which of the following is the LARGEST MTU for a standard Ethernet frame?

- A. 1452
- B. 1492
- C. 1500
- D. 2304

Answer: C

Explanation:

The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

https://en.wikipedia.org/wiki/Maximum_transmission_unit

NEW QUESTION 33

SIMULATION - (Topic 1)

SIMULATION

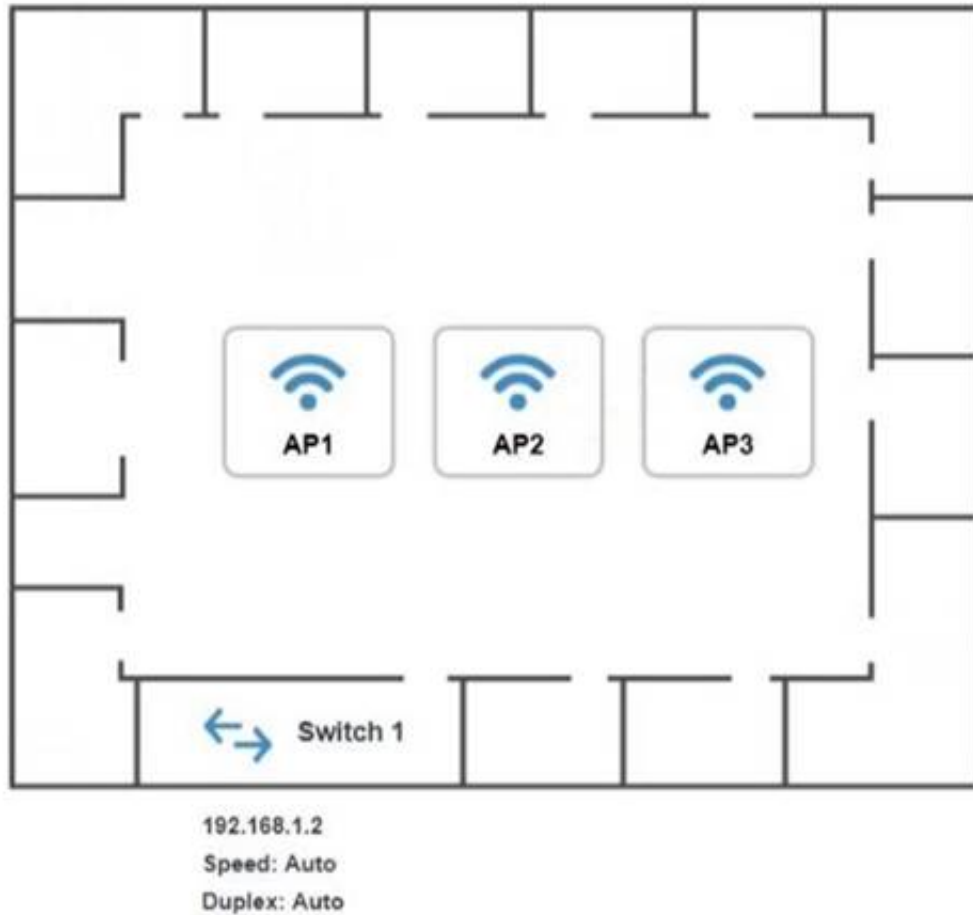
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t! The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS

Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes
 ☐ No

Wireless

Mode

B

G

Channel

Wired

Speed

☐ Auto
 ☒ 100
 ☐ 1000

Duplex

☐ Auto
 ☐ Half
 ☒ Full

Security Configuration

Security Settings

☒ None
 ☐ WEP
 ☐ WPA
 ☐ WPA2
 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

Yes

No

Wireless

Mode

B

G

Channel

1

2

3

4

5

6

7

8

9

10

11

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

B

G

Channel

1

2

3

4

5

6

7

8

9

10

11

Wired

Speed

☐ Auto

☒ 100

☐ 1000

Duplex

☐ Auto

☐ Half

☒ Full

Security Configuration

Security Settings

☒ None

☐ WEP

☐ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

On the first exhibit, the layout should be as follows

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

192.168.1.32

/

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

3

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Graphical user interface, text, application, chat or text message Description automatically generated
Description automatically generated

AP1 Configuration

https://ap1.setup.do

IP Address

192.168.1.32

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

3

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Graphical user interface
Description automatically generated

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Graphical user interface, text, application, chat or text message
Description automatically generated

The Leader of IT Certification

visit - <https://www.certleader.com>

AP1 Configuration

←

→

↺

https://ap1.setup.do

IP Address

192.168.1.3 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes
 ☐ No

Wireless

Mode

G

Channel

3

Wired

Speed

☒ Auto
 ☐ 100
 ☐ 1000

Duplex

☒ Auto
 ☐ Half
 ☐ Full

Security Configuration

Security Settings

☐ None
 ☐ WEP
 ☒ WPA
 ☐ WPA2
 ☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Graphical user interface
Description automatically generated
Exhibit 2 as follows
Access Point Name AP2

AP2 Configuration

←

→

↺

https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

192.168.1.64 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes
 ☐ No

Wireless

Mode

B

Channel

6

Wired

Speed

☐ Auto
 ☒ 100
 ☐ 1000

Duplex

☐ Auto
 ☐ Half
 ☒ Full

Security Configuration

Reset to Default

Save

Close

Graphical user interface
Description automatically generated

Security Configuration

Security Settings

☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Graphical user interface, text, application, chat or text message
Description automatically generated

AP2 Configuration

←

→

↺

https://ap2.setup.do

IP Address

192.168.1.4 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

G

Channel

6

Wired

Speed

☒ Auto ☐ 100 ☐ 1000

Duplex

☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings

☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Graphical user interface
Description automatically generated
Exhibit 3 as follows
Access Point Name AP3

The Leader of IT Certification

visit - <https://www.certleader.com>

AP3 Configuration

←

→

↺

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

192.168.1.96

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

B

▼

Channel

9

▼

Wired

Speed

☐ Auto

☒ 100

☐ 1000

Duplex

☐ Auto

☐ Half

☒ Full

Security Configuration

Reset to Default

Save

Close

Graphical user interface
Description automatically generated

Security Configuration

Security Settings

☐ None

☐ WEP

☐ WPA

☐ WPA2

☒ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Graphical user interface, text, application, chat or text message
Description automatically generated

AP3 Configuration

←

→

↺

https://ap3.setup.do

IP Address

192.168.1.5

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

G

▼

Channel

9

▼

Wired

Speed

☒ Auto

☐ 100

☐ 1000

Duplex

☒ Auto

☐ Half

☐ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☒ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Graphical user interface
Description automatically generated

NEW QUESTION 35

- (Topic 1)

A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment. Which of the following will allow the technician to record these changes?

- A. Asset tags
- B. A smart locker
- C. An access control vestibule
- D. A camera

Answer: A

Explanation:

Asset tags will allow the technician to record changes to new and old equipment when installing multiple UPS units in a major retail store. Asset tags are labels or stickers that are attached to physical assets such as computers, printers, servers, or UPS units. They usually contain information such as asset name, serial number, barcode, QR code, or RFID chip that can be scanned or read by an asset management system or software. Asset tags help track inventory, location, status, maintenance, and ownership of assets. References: <https://www.camcode.com/asset-tags/asset-tagging-guide/>

NEW QUESTION 40

- (Topic 1)

Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

- A. Install load balancers
- B. Install more switches
- C. Decrease the number of VLANs
- D. Reduce the lease time

Answer: D

Explanation:

To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.

References:

? CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.

? <https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance>

NEW QUESTION 44

- (Topic 1)

Which of the following connector types would have the MOST flexibility?

- A. SFP
- B. BNC
- C. LC
- D. RJ45

Answer: A

Explanation:

SFP (Small Form-factor Pluggable) is a connector type that has the most flexibility. It is a hot-swappable transceiver that can support different speeds, distances, and media types depending on the module inserted. It can be used for both copper and fiber connections and supports various protocols such as Ethernet, Fibre Channel, and SONET. References: <https://www.fs.com/what-is-sfp-transceiver-aid-11.html>

NEW QUESTION 48

- (Topic 1)

A technician wants to deploy a new wireless network that comprises 30 WAPs installed throughout a three-story office building. All the APs will broadcast the same SSID for client access. Which of the following BEST describes this deployment?

- A. Extended service set
- B. Basic service set
- C. Unified service set
- D. Independent basic service set

Answer: A

Explanation:

An extended service set (ESS) is a wireless network that consists of multiple access points (APs) that share the same SSID and are connected by a wired network. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity. A basic service set (BSS) is a wireless network that consists of a single AP and its associated clients. An independent basic service set (IBSS) is a wireless network that consists of a group of clients that communicate directly without an AP. A unified service set is not a standard term for a wireless network. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), [https://en.wikipedia.org/wiki/Service_set_\(802.11_network\)](https://en.wikipedia.org/wiki/Service_set_(802.11_network))

NEW QUESTION 52

- (Topic 2)

A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other. Which of the following would BEST accomplish this requirement?

- A. Wireless client isolation

- B. Port security
- C. Device geofencing
- D. DHCP snooping

Answer: A

Explanation:

Wireless client isolation is a feature on wireless routers that limits the connectivity between wireless devices connected to the same network. It prevents them from accessing resources on other wireless or wired devices, as a security measure to reduce attacks and threats. This feature can be useful for guest and BYOD SSIDs, but it can also be disabled on the router's settings. References: <https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option/>

NEW QUESTION 54

- (Topic 2)

A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

- A. Mandatory access control
- B. User-based permissions
- C. Role-based access
- D. Least privilege

Answer: C

Explanation:

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

NEW QUESTION 56

- (Topic 2)

Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

- A. Storage array
- B. Type 1 hypervisor
- C. Virtual machine
- D. Guest QS

Answer: B

Explanation:

A type 1 hypervisor is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines. A hypervisor is a software layer that enables virtualization by creating and managing virtual machines (VMs) on a physical host. A type 1 hypervisor, also known as a bare-metal hypervisor or a native hypervisor, runs directly on the host's hardware without requiring an underlying operating system (OS). It provides better performance and security than a type 2 hypervisor, which runs on top of an existing OS and relies on it for hardware access. References: <https://www.vmware.com/topics/glossary/content/hypervisor>

NEW QUESTION 58

- (Topic 2)

Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

- A. DDoS
- B. Phishing
- C. Ransomware
- D. MAC spoofing

Answer: C

Explanation:

Ransomware is a type of malware that encrypts user data and demands a ransom for its decryption. Ransomware can prevent users from accessing their files and applications, and cause data loss or corruption. A proper backup implementation is essential to recover from a ransomware attack, as it can help restore the encrypted data without paying the ransom or relying on the attackers' decryption key. References: <https://www.comptia.org/blog/what-is-ransomware>

NEW QUESTION 62

- (Topic 2)

A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

- A. 10GBaseT
- B. 1000BaseT
- C. 1000BaseSX
- D. 1000BaseLX

Answer: C

Explanation:

1000BaseSX is an Ethernet standard that should be used to connect the network switch to the existing multimode fiber optic cable. 1000BaseSX is a Gigabit Ethernet standard that uses short-wavelength laser (850 nm) over multimode fiber optic cable. It can support distances up to 550 meters depending on the cable type and quality. It is suitable for short-range network segments such as campus or building backbone networks. References: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product_data_sheet09186a008014cb5e.html

NEW QUESTION 66

- (Topic 2)

An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

- A. nslookup
- B. show config
- C. netstat
- D. show interface
- E. show counters

Answer: D

Explanation:

show interface is a command-line tool that displays information about the status, configuration, and statistics of an interface on a network device. A technician can use show interface to determine where the incident is occurring in a network by checking the uplink status, speed, duplex mode, errors, collisions, and other parameters of each interface. References: <https://www.comptia.org/blog/what-is-show-interface>

NEW QUESTION 67

- (Topic 2)

An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology Which of the following is the number of additional network connections needed?

- A. 5
- B. 7
- C. 10
- D. 15

Answer: C

Explanation:

10 additional network connections are needed to transition from a star to a full-mesh topology. A star topology is a network topology where each device is connected to a central device, such as a switch or a hub. A full-mesh topology is a network topology where each device is directly connected to every other device. The number of connections needed for a full-mesh topology can be calculated by the formula $n(n-1)/2$, where n is the number of devices. In this case, there are six devices (one core and five distribution switches), so the number of connections needed for a full-mesh topology is $6(6-1)/2 = 15$. Since there are already five connections in the star topology (one from each distribution switch to the core switch), the number of additional connections needed is $15 - 5 = 10$. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 70

- (Topic 2)

A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC After checking the is setting, the technician found the DNS server address was incorrect Which of the following describes the issue?

- A. Rogue DHCP server
- B. Misconfigured HSRP
- C. DNS poisoning
- D. Exhausted IP scope

Answer: C

Explanation:

DNS poisoning is a type of attack that modifies the DNS records of a domain name to point to a malicious IP address instead of the legitimate one. This can result in users being directed to cloned websites that are stealing credentials, even if they enter the correct URL for the website. The incorrect DNS server address on the user's PC could be a sign of DNS poisoning, as the attacker could have compromised the DNS server or spoofed its response to redirect the user's queries. References: <https://www.comptia.org/blog/what-is-dns-poisoning>

NEW QUESTION 74

- (Topic 2)

A network administrator is downloading a large patch that will be uploaded to several enterprise switches simultaneously during the day's upgrade cycle. Which of the following should the administrator do to help ensure the upgrade process will be less likely to cause problems with the switches?

- A. Confirm the patch's MD5 hash prior to the upgrade
- B. Schedule the switches to reboot after an appropriate amount of time.
- C. Download each switch's current configuration before the upgrade
- D. Utilize FTP rather than TFTP to upload the patch

Answer: A

Explanation:

The network administrator should confirm the patch's MD5 hash prior to the upgrade to help ensure the upgrade process will be less likely to cause problems with the switches. MD5 (Message Digest 5) is a cryptographic hash function that produces a 128-bit hash value for any given input. It can be used to verify the integrity and authenticity of a file by comparing its hash value with a known or expected value. If the hash values match, it means that the file has not been corrupted or

tampered with during transmission or storage. If the hash values do not match, it means that the file may be damaged or malicious and should not be used for the upgrade. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html>

NEW QUESTION 75

- (Topic 2)

A network administrator needs to implement an HDMI over IP solution. Which of the following will the network administrator MOST likely use to ensure smooth video delivery?

- A. Link aggregation control
- B. Port tagging
- C. Jumbo frames
- D. Media access control

Answer: C

Explanation:

Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

NEW QUESTION 79

- (Topic 2)

A network administrator decided to use SLAAC in an extensive IPv6 deployment to alleviate IP address management. The devices were properly connected into the LAN but autoconfiguration of the IP address did not occur as expected. Which of the following should the network administrator verify?

- A. The network gateway is configured to send router advertisements.
- B. A DHCP server is present on the same broadcast domain as the clients.
- C. The devices support dual stack on the network layer.
- D. The local gateway supports anycast routing.

Answer: A

Explanation:

SLAAC (Stateless Address Autoconfiguration) is a method for IPv6 devices to automatically configure their IP addresses based on the network prefix advertised by a router. The router sends periodic router advertisements (RAs) that contain the network prefix and other parameters for the devices to use. If the network gateway is not configured to send RAs, then SLAAC will not work. A DHCP server is not needed for SLAAC, as the devices generate their own addresses without relying on a server. Dual stack and anycast routing are not related to SLAAC.

NEW QUESTION 80

- (Topic 2)

A network field technician is installing and configuring a secure wireless network. The technician performs a site survey. Which of the following documents would MOST likely be created as a result of the site survey?

- A. Physical diagram
- B. Heat map
- C. Asset list
- D. Device map

Answer: B

Explanation:

A heat map would most likely be created as a result of the site survey. A heat map is a graphical representation of the wireless signal strength and coverage in a given area. It can show the location of APs, antennas, walls, obstacles, interference sources, and dead zones. It can help with planning, optimizing, and troubleshooting wireless networks. References: <https://www.netspotapp.com/what-is-a-wifi-heatmap.html>

NEW QUESTION 84

- (Topic 2)

A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

- A. Secure SNMP
- B. Port security
- C. Implicit deny
- D. DHCP snooping

Answer: C

Explanation:

Implicit deny is a firewall rule that blocks all traffic that is not explicitly allowed by other rules. Implicit deny is usually applied as the last rule in the firewall to ensure that only the necessary access requirements are allowed through the firewall and that any unwanted or malicious traffic is rejected. Implicit deny can also provide a default security policy and a baseline for auditing and logging purposes.

Secure SNMP is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis. Secure SNMP can be used to monitor and manage the status, performance, and configuration of network devices. Secure SNMP can also help to detect and respond to potential problems or faults on the network. However, secure SNMP is not a firewall rule; it is a network management protocol.

Port security is a feature that allows a switch to restrict the devices that can connect to a specific port based on their MAC addresses. Port security can help to prevent unauthorized access, spoofing, or MAC flooding attacks on the switch. However, port security is not a firewall rule; it is a switch feature. DHCP snooping is a feature that allows a switch to filter DHCP messages and prevent rogue DHCP servers from assigning IP addresses to devices on the network. DHCP snooping can help to prevent IP address conflicts, spoofing, or denial-of-service attacks on the network. However, DHCP snooping is not a firewall rule; it is a switch feature.

NEW QUESTION 89

- (Topic 2)

A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall Which of the following would be the MOST appropriate way to enable secure remote printing?

- A. SSH
- B. VPN
- C. Telnet
- D. SSL

Answer: B

Explanation:

VPN (Virtual Private Network) is the most appropriate way to enable secure remote printing. VPN is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. VPN can be used for various purposes such as accessing corporate resources, bypassing geo-restrictions, or enhancing privacy and security. VPN can also be used for remote printing by allowing users to connect to a printer on the private network and send print jobs securely over the VPN tunnel. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>

NEW QUESTION 91

- (Topic 2)

Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

- A. Session
- B. Physical
- C. Presentation
- D. Data link

Answer: A

Explanation:

Reference: <https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and%20terminates%20conversations%20between%20applications.>

The session layer is where conversations between applications are established, coordinated, and terminated. It is responsible for creating, maintaining, and ending sessions between different devices or processes. The physical layer deals with the transmission of bits over a medium. The presentation layer formats and translates data for different applications. The data link layer provides reliable and error-free delivery of frames within a network.

NEW QUESTION 96

- (Topic 2)

Which of the following policies is MOST commonly used for guest captive portals?

- A. AUP
- B. DLP
- C. BYOD
- D. NDA

Answer: A

Explanation:

AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. References: https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal.htm

NEW QUESTION 100

- (Topic 2)

A network technician is investigating an issue with a desktop that is not connecting to the network. The desktop was connecting successfully the previous day, and no changes were made to the environment. The technician locates the switchport where the device is connected and observes the LED status light on the switchport is not lit even though the desktop is turned on Other devices that are plugged into the switch are connecting to the network successfully Which of the following is MOST likely the cause of the desktop not connecting?

- A. Transceiver mismatch
- B. VLAN mismatch
- C. Port security
- D. Damaged cable
- E. Duplex mismatch

Answer: D

Explanation:

A damaged cable is most likely the cause of the desktop not connecting to the network. A damaged cable can cause physical layer issues such as loss of signal, attenuation, interference, or crosstalk. These issues can prevent the desktop from establishing a link with the switch and result in the LED status light on the switchport being off. Other possible causes of physical layer issues are faulty connectors, ports, or transceivers. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/14119-37.html>

NEW QUESTION 102

- (Topic 2)

An ARP request is broadcasted and sends the following request. "Who is 192.168.1.200?"

Tell 192.168.1.55"

At which of the following layers of the OSI model does this request operate?

- A. Application
- B. Data link
- C. Transport
- D. Network
- E. Session

Answer: B

Explanation:

An ARP request operates at the data link layer of the OSI model. ARP (Address Resolution Protocol) is a protocol that maps IP addresses to MAC addresses on a local area network. It allows devices to communicate with each other without knowing their MAC addresses beforehand. ARP operates at the data link layer (layer 2) of the OSI model, which is responsible for framing and addressing data packets on a physical medium. References:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 105

- (Topic 2)

A corporation has a critical system that would cause unrecoverable damage to the brand if it was taken offline. Which of the following disaster recovery solutions should the corporation implement?

- A. Full backups
- B. Load balancing
- C. Hot site
- D. Snapshots

Answer: C

Explanation:

A hot site is the disaster recovery solution that the corporation should implement for its critical system that would cause unrecoverable damage to the brand if it was taken offline. A hot site is a fully operational backup site that can take over the primary site's functions in case of a disaster or disruption. A hot site has all the necessary hardware, software, data, network connections, and personnel to resume normal operations with minimal downtime. A hot site is suitable for systems that require high availability and cannot afford any data loss or interruption. References: <https://www.enterprisestorageforum.com/management/disaster-recovery-site/> 1

NEW QUESTION 110

- (Topic 2)

A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

- A. Port security
- B. Local authentication
- C. TACACS+
- D. Access control list

Answer: C

Explanation:

TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve the security of the management console on the company's switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. References:

<https://www.comptia.org/blog/what-is-tacacs>

NEW QUESTION 114

- (Topic 2)

A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

- A. Standard operating procedures
- B. Configuration baseline documents
- C. Work instructions
- D. Change management documentation

Answer: D

Explanation:

Change management documentation is a record of the changes that have been made to a system or process, including the reason, date, time, and impact of each change. A technician can reference this documentation to find what solution was implemented to resolve a previously encountered issue, as well as any potential side effects or dependencies of the change. References: <https://www.comptia.org/blog/what-is-change-management>

NEW QUESTION 118

- (Topic 2)

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the

AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

Answer: A

Explanation:

An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP1. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION 121

- (Topic 2)

Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

- A. Vulnerability assessment
- B. Factory reset
- C. Firmware update
- D. Screened subnet

Answer: C

Explanation:

Firmware is a type of software that controls the low-level functions of a hardware device, such as a router, switch, printer, or camera. Firmware updates are patches or upgrades that fix bugs, improve performance, add features, or address security vulnerabilities in firmware. Firmware updates are commonly used to address CVEs (Common Vulnerabilities and Exposures) on network equipment and operating systems, as CVEs are publicly known flaws that can be exploited by attackers. References: <https://www.comptia.org/blog/what-is-firmware>

NEW QUESTION 123

- (Topic 3)

Which of the following describes traffic going in and out of a data center from the internet?

- A. Demarcation point
- B. North-South
- C. Fibre Channel
- D. Spine and leaf

Answer: B

NEW QUESTION 125

- (Topic 3)

While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues. Which of the following is MOST likely the cause of the low data rate and port errors?

- A. Bad switch ports
- B. Duplex issues
- C. Cable length
- D. Incorrect pinout

Answer: B

NEW QUESTION 126

- (Topic 3)

Which of the following devices would be used to extend the range of a wireless network?

- A. A repeater
- B. A media converter
- C. A router
- D. A switch

Answer: A

Explanation:

A repeater is a device used to extend the range of a wireless network by receiving, amplifying, and retransmitting wireless signals. It is typically used to extend the range of a wireless network in a large area, such as an office building or a campus. Repeaters can also be used to connect multiple wireless networks together, allowing users to move seamlessly between networks. As stated in the CompTIA Network+ Study Manual, "a wireless repeater is used to extend the range of a wireless network by repeating the signal from one access point to another."

NEW QUESTION 128

- (Topic 3)

A network engineer designed and implemented a new office space with the following characteristics:

Building construction type:	Brick
Layout:	10,764sq ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

One month after the office space was implemented, users began reporting dropped signals when entering another room and overall poor connections to the 5GHz network. 'which of the following should the engineer do to best resolve the issue?

- A. use non-overlapping channels
- B. Reconfigure the network to support 2.4GHz_
- C. Upgrade to WPA3.
- D. Change to directional antennas-

Answer: D

Explanation:

The best solution to resolve the issue of dropped signals and poor connections to the 5GHz network is to change to directional antennas. Directional antennas are antennas that focus the wireless signal in a specific direction, increasing the range and strength of the signal. Directional antennas are suitable for environments where there are obstacles or interference that can weaken or block the wireless signal. In the image, the office space has several walls and doors that can reduce the signal quality of the 5GHz network, which has a shorter wavelength and higher frequency than the 2.4GHz network. By using directional antennas, the network engineer can aim the wireless signal towards the desired areas and avoid the signal loss caused by the walls and doors. References: CompTIA Network+ N10-008 Certification Study Guide, page 76; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-19.

NEW QUESTION 132

- (Topic 3)

An IT administrator is creating an alias to the primary customer's domain. Which of the following DNS record types does this represent?

- A. CNAME
- B. MX
- C. A
- D. PTR

Answer: A

Explanation:

A CNAME record is a type of DNS record that maps an alias name to a canonical name, or the primary domain name. A CNAME record is used to create subdomains or alternative names for the same website, without having to specify the IP address for each alias. For example, a CNAME record can map www.example.com to example.com, or mail.example.com to example.com. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.4

NEW QUESTION 136

- (Topic 3)

A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected for the VPN connection. Which of the following will MOST likely point to the root cause of the Issue?

- A. Checking the routing tables on both sides to ensure there is no asymmetric routing
- B. Checking on the partner network for a missing route pointing to the VPN connection
- C. Running iPerf on both sides to confirm the delay that is measured is accurate
- D. Checking for an incorrect VLAN assignment affecting the MPLS traffic

Answer: A

Explanation:

Asymmetric routing can occur when two routers have different paths for the same two hosts, resulting in increased latency and possible packet loss. According to the CompTIA Network+ Study Manual, "If the path from the source to the destination is not the same in both directions, the packets will take different routes and the latency can increase significantly." To confirm this, the network administrator should check the routing tables on both sides of the connection and ensure that the same path is used in both directions.

NEW QUESTION 138

- (Topic 3)

Which of the following routing technologies is used to prevent network failure at the gateway by protecting data traffic from a failed router?

- A. BGP
- B. OSPF
- C. EIGRP
- D. FHRP

Answer: D

Explanation:

FHRP stands for First Hop Redundancy Protocol, and it is a group of protocols that allow routers to work together to provide backup or failover for the default gateway in a network. FHRP can prevent network failure at the gateway by protecting data traffic from a failed router and ensuring that there is always an active router to forward packets. Some examples of FHRP protocols are HSRP, VRRP, and GLBP12.

References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 13: Routing Protocols32: First Hop Redundancy Protocols (FHRP) Explained4

NEW QUESTION 140

- (Topic 3)

A customer connects a firewall to an ISP router that translates traffic destined for the internet. The customer can connect to the internet but not to the remote site. Which of the following will verify the status of NAT?

- A. tcpdump
- B. nmap
- C. ipconfig
- D. tracer

Answer: A

Explanation:

tcpdump is a command-line tool that can capture and analyze network traffic on a given interface. tcpdump can verify the status of NAT by showing the source and destination IP addresses of the packets before and after they pass through the ISP router that translates traffic destined for the internet. tcpdump can also show the NAT protocol and port numbers used by the router. nmap, ipconfig, and tracer are not suitable tools for verifying the status of NAT, as they do not show the IP address translation process.

References

- ? 1: Network Address Translation – N10-008 CompTIA Network+ : 1.4
- ? 2: CompTIA Network+ N10-008 Certification Study Guide, page 95-96
- ? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 16
- ? 4: CompTIA Network+ N10-008 Certification Practice Test, question 7

NEW QUESTION 145

- (Topic 3)

Which of the following, in addition to a password, can be asked of a user for MFA?

- A. PIN
- B. Favorite color
- C. Hard token
- D. Mother's maiden name

Answer: A

Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying the identity of a user by requiring two or more pieces of evidence that belong to different categories: something the user knows, something the user has, or something the user is. A password is something the user knows, and it is usually combined with another factor such as a PIN (Personal Identification Number) or a hard token (a physical device that generates a one- time code) that the user has. A favorite color or a mother's maiden name are not suitable for MFA, as they are also something the user knows and can be easily guessed or compromised.

References

- ? 1: Multi-Factor Authentication – N10-008 CompTIA Network+ : 3.1
- ? 2: CompTIA Network+ Certification Exam Objectives, page 13
- ? 3: CompTIA Network+ N10-008 Certification Study Guide, page 250
- ? 4: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 14

NEW QUESTION 148

- (Topic 3)

Which of the following BEST describes a north-south traffic flow?

- A. A public internet user accessing a published web server
- B. A database server communicating with another clustered database server
- C. A Layer 3 switch advertising routes to a router
- D. A management application connecting to managed devices

Answer: A

Explanation:

A north-south traffic flow is a term used to describe the communication between a user or device outside the network and a server or service inside the network. For example, a public internet user accessing a published web server is a north-south traffic flow. This type of traffic flow typically crosses the network perimeter and requires security measures such as firewalls and VPNs. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1- 9.

North-south traffic flow refers to the flow of traffic between the internal network of an organization and the external world. This type of traffic typically flows from the internet to the organization's internal network, and back again.

Examples of north-south traffic flow include:

- ? A public internet user accessing a published web server
- ? A remote employee connecting to a VPN
- ? An email client sending email to an external server
- ? A customer connecting to an e-commerce website

References:

- ? CompTIA Network+ N10-008 Exam Objectives, Version 5.0, August 2022, page 12
- ? CompTIA Network+ Certification Study Guide, Seventh Edition, Todd Lammle, Sybex, 2022, page 17

NEW QUESTION 150

- (Topic 3)

A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

- A. An IPS
- B. A Layer 3 switch
- C. A router
- D. A wireless LAN controller

Answer: B

NEW QUESTION 153

- (Topic 3)

Which of the following fiber connector types is the most likely to be used on a network interface card?

- A. LC
- B. SC
- C. ST
- D. MPO

Answer: A

Explanation:

LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network¹².

References:

? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11

? CompTIA Network+ Certification Exam Objectives²

NEW QUESTION 154

- (Topic 3)

Users in a branch can access an In-house database server, but it is taking too long to fetch records. The analyst does not know whether the issue is being caused by network latency. Which of the following will the analyst MOST likely use to retrieve the metrics that are needed to resolve this issue?

- A. SNMP
- B. Link state
- C. Syslog
- D. QoS
- E. Traffic shaping

Answer: A

NEW QUESTION 157

- (Topic 3)

Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

- A. Use a media converter and a UTP cable
- B. Install an additional transceiver module and use GBICs
- C. Change the type of connector from SC to F-type
- D. Use a loopback adapter to make the connection

Answer: A

NEW QUESTION 160

- (Topic 3)

Which of the following is most likely to be implemented to actively mitigate intrusions on a host device?

- A. HIDS
- B. MDS
- C. HIPS
- D. NIPS

Answer: A

Explanation:

HIDS (host-based intrusion detection system) is a type of security software that monitors and analyzes the activity on a host device, such as a computer or a server. HIDS can detect and alert on intrusions, such as malware infections, unauthorized access, configuration changes, or policy violations. HIDS can also actively mitigate intrusions by blocking or quarantining malicious processes, files, or network connections¹.

HIPS (host-based intrusion prevention system) is similar to HIDS, but it can also prevent intrusions from happening in the first place by enforcing security policies and rules on the host device². MDS (multilayer switch) is a network device that combines the functions of a switch and a router, and it does not directly protect a host device from intrusions³. NIPS (network-based intrusion prevention system) is a network device that monitors and blocks malicious traffic on the network level, and it does not operate on the host device level⁴.

NEW QUESTION 165

- (Topic 3)

A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

- A. Ethernet cable type
- B. Voltage
- C. Transceiver compatibility
- D. DHCP addressing

Answer: B

Explanation:

The most likely reason why only eight cameras turn on is that the PoE switch does not have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.

References:

? CompTIA Network+ N10-008 Certification Study Guide, page 181

? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352

? PoE Troubleshooting: The Common PoE Errors and Solutions3

NEW QUESTION 170

- (Topic 3)

Which of the following documents is MOST likely to be associated with identifying and documenting critical applications?

- A. Software development life-cycle policy
- B. User acceptance testing plan
- C. Change management policy
- D. Business continuity plan

Answer: D

Explanation:

A business continuity plan (BCP) is a document that outlines the procedures and strategies to ensure the continuity of critical business functions in the event of a disaster or disruption. A BCP is most likely to be associated with identifying and documenting critical applications that are essential for the organization's operations and recovery. A BCP also defines the roles and responsibilities of the staff, the backup and restore processes, the communication channels, and the testing and maintenance schedules.

References: Network+ Study Guide Objective 5.2: Explain disaster recovery and business continuity concepts.

NEW QUESTION 174

- (Topic 3)

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/21
- B. 10.0.0.0/22
- C. 10.0.0.0/23
- D. 10.0.0.0/24

Answer: B

NEW QUESTION 178

- (Topic 3)

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not come on. Which of the following should a technician try first to troubleshoot this issue?

- A. Reverse the fibers.
- B. Rerterminate the fibers.
- C. Verify the fiber size.
- D. Examine the cable runs for visual faults.

Answer: A

Explanation:

One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission12.

To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly12. The other options are not the first steps to troubleshoot this issue. Rerterminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

NEW QUESTION 182

- (Topic 3)

A technician is expanding a wireless network and adding new access points. The company requires that each access point broadcast the same SSID. Which of the following should the technician implement for this requirement?

- A. MIMO
- B. Roaming
- C. Channel bonding
- D. Extended service set

Answer: D

Explanation:

An extended service set (ESS) is a wireless network that consists of two or more access points (APs) that share the same SSID and are connected by a distribution system, such as a switch or a router. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity or changing network settings. An ESS can also increase the coverage area and capacity of a wireless network

NEW QUESTION 186

- (Topic 3)

During the troubleshooting of an E1 line, the point-to-point link on the core router was accidentally unplugged and left unconnected for several hours. However, the network management team was not notified. Which of the following could have been configured to allow early detection and possible resolution of the issue?

- A. Traps
- B. MIB
- C. OID
- D. Baselines

Answer: A

Explanation:

Traps are unsolicited messages sent by network devices to a network management system (NMS) when an event or a change in status occurs. Traps can help notify the network management team of any issues or problems on the network, such as a link failure or a device reboot. Traps can also trigger actions or alerts on the NMS, such as sending an email or logging the event. MIB stands for Management Information Base and is a database of information that can be accessed and managed by an NMS using SNMP (Simple Network Management Protocol). OID stands for Object Identifier and is a unique name that identifies a specific variable in the MIB. Baselines are measurements of normal network performance and behavior that can be used for comparison and analysis. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION 188

- (Topic 3)

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools would help identify which ports are open on the remote file server?

- A. dig
- B. nmap
- C. tracert
- D. nslookup

Answer: B

Explanation:

nmap is the tool that would help identify which ports are open on the remote file server. nmap stands for Network Mapper, which is a free and open-source tool that can perform various network scanning and discovery tasks. nmap can help identify which ports are open on a remote device by sending probes or packets to different ports and analyzing the responses. nmap can also provide information about the operating system, services, versions, firewalls, or vulnerabilities of the remote device. nmap can be useful for network administrators, security professionals, or hackers to monitor, audit, or attack network devices. References: [CompTIA Network+ Certification Exam Objectives], Nmap - Free Security Scanner For Network Exploration & Security Audits

NEW QUESTION 193

- (Topic 3)

A customer needs six usable IP addresses. Which of the following best meets this requirement?

- A. 255.255.255.128
- B. 255.255.255.192
- C. 255.255.255.224
- D. 255.255.255.240

Answer: C

NEW QUESTION 197

- (Topic 3)

A company streams video to multiple devices across a campus. When this happens, several users report a degradation of network performance. Which of the following would MOST likely address this issue?

- A. Enable IGMP snooping on the switches.
- B. Implement another DHCP server.
- C. Reconfigure port tagging for the video traffic.
- D. Change the SSID of the APs

Answer: A

NEW QUESTION 202

- (Topic 3)

Which of the following can be used to store various types of devices and provide contactless delivery to users?

- A. Asset tags
- B. Biometrics
- C. Access control vestibules
- D. Smart lockers

Answer: D

NEW QUESTION 207

- (Topic 3)

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

```
Tracing route to 10.10.0.22 over a maximum of 30 hops:
 0  14ms  20ms  15ms  192.168.1.253
 1  10ms  15ms  12ms  172.16.0.21
 2   5ms   10ms  10ms  10.10.5.3
 3  10ms  15ms  12ms  10.12.2.1
 4   5ms   10ms  10ms  10.10.5.3
 5  10ms  15ms  12ms  10.12.2.1
 6   5ms   10ms  10ms  10.10.5.3
 7  10ms  15ms  12ms  10.12.2.1
```

Which of the following is the cause of the connection issue?

- A. Routing loop
- B. Asymmetrical routing
- C. Broadcast storm
- D. Switching loop

Answer: A

Explanation:

The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. References: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

NEW QUESTION 209

- (Topic 3)

A large metropolitan city is looking to standardize the ability for police department laptops to connect to the city government's VPN. The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers. Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

- A. 5G
- B. LTE
- C. Wi-Fi 4
- D. Wi-Fi 5
- E. Wi-Fi 6

Answer: B

NEW QUESTION 213

- (Topic 3)

After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:

Which of the following is the most likely issue?

- A. Packet loss
- B. Bottlenecking
- C. Channel overlap
- D. Network congestion

Answer: B

Explanation:

The most likely issue is bottlenecking. Bottlenecking occurs when a component or device limits the performance or capacity of the network. In this case, the IPS (intrusion prevention system) may be causing a bottleneck by inspecting and filtering the incoming and outgoing traffic, which reduces the speed and bandwidth available for the network devices.

To confirm this issue, the network administrator can compare the speed test results before and after installing the IPS, and check the IPS configuration and logs for any errors or warnings. The network administrator can also try to bypass the IPS temporarily and run the speed test again to see if there is any improvement.

If the IPS is indeed the cause of the bottleneck, the network administrator can try to optimize the IPS settings, such as adjusting the inspection rules, thresholds, and priorities, to reduce the processing overhead and latency. Alternatively, the network administrator can upgrade the IPS hardware or software, or add more IPS devices to balance the load and increase the throughput.

1: What is Network Congestion? Common Causes and How to Fix Them? -

GeeksforGeeks 2: Network congestion - Wikipedia 3: How to Fix Packet Loss - Lifewire 4: How to Optimize Your IPS Performance - Cisco 5: How to Avoid Network Bottlenecks - TechRepublic

NEW QUESTION 216

- (Topic 3)

Which of the following types of connections would need to be set up to provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols?

- A. Client-to-site VPN
- B. Clientless VPN
- C. RDP
- D. Site-to-site VPN
- E. SSH

Answer: D

NEW QUESTION 220

- (Topic 3)

Which of the following describes when an active exploit is used to gain access to a network?

- A. Penetration testing
- B. Vulnerability testing
- C. Risk assessment
- D. Posture assessment
- E. Baseline testing

Answer: A

Explanation:

Penetration testing is a type of security testing that is used to assess the security of a system or network by actively exploiting known vulnerabilities. It is used to simulate an attack on the system and identify any weaknesses that may be exploited by malicious actors. As stated in the CompTIA Security+ Study Guide, "penetration testing is a type of security assessment that attempts to gain unauthorized access to networks and systems by exploiting security vulnerabilities."

NEW QUESTION 223

SIMULATION - (Topic 3)

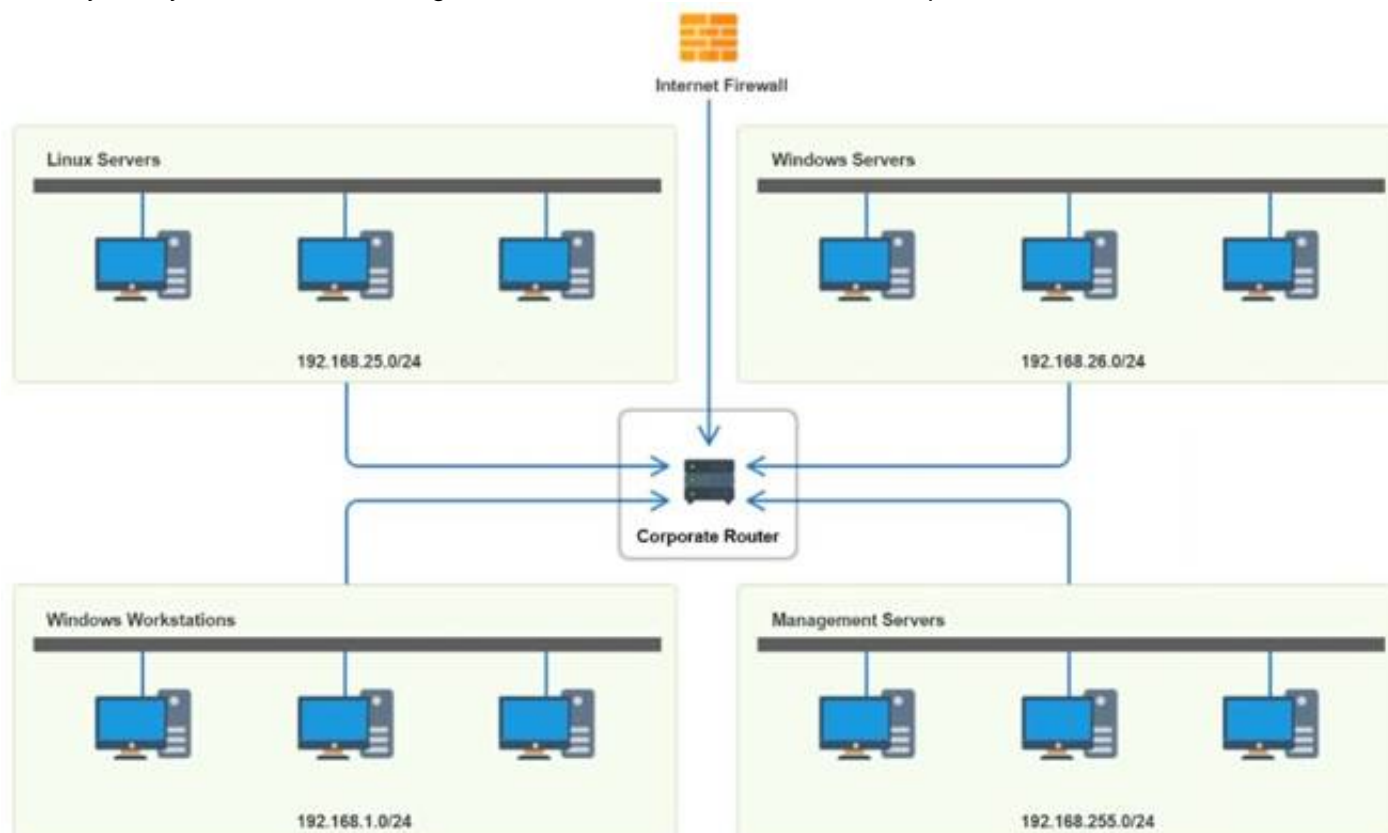
You have been tasked with implementing an ACL on the router that will:

- * 1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
- * 2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
- * 3. Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Router Access Control List ✕					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

NEW QUESTION 225

- (Topic 3)

A network administrator is configuring a firewall to allow for a new cloud-based email server. The company standard is to use SMTP to route email traffic. Which of the following ports, by default, should be reserved for this purpose?

- A. 23
- B. 25
- C. 53
- D. 110

Answer: B

Explanation:

Port 25, by default, should be reserved for SMTP traffic to allow for a new cloud-based email server. SMTP stands for Simple Mail Transfer Protocol, which is a network protocol that enables email communication between mail servers and clients. SMTP uses port 25 as its default port for sending and receiving email messages over TCP/IP networks. A cloud-based email server is an email server that is hosted on a cloud service provider's infrastructure, rather than on-premise or in-house. A cloud-based email server can offer advantages such as scalability, reliability, security, and cost-effectiveness. To allow for a new cloud-based email server, a firewall should be configured to open port 25 for SMTP traffic. References: [CompTIA Network+ Certification Exam Objectives], What Is SMTP? | Mailtrap Blog, Cloud Email Server: What Is It & How Does It Work? | Zoho Mail

NEW QUESTION 229

- (Topic 3)

Which of the following protocols should be used when Layer 3 availability is of the highest concern?

- A. LACP
- B. LDAP
- C. FHRP
- D. DHCP

Answer: C

Explanation:

FHRP stands for First Hop Redundancy Protocol, which is a group of protocols that allow routers or switches to provide backup or failover for the default gateway in a network. FHRP ensures that the network traffic can reach its destination even if the primary gateway fails or becomes unavailable. Some examples of FHRP protocols are HSRP, VRRP, and GLBP.

References

- ? 1: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 18
- ? 2: CompTIA Network+ N10-008 Certification Practice Test, question 9
- ? 3: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 263
- ? 4: CompTIA Network+ (N10-008) Practice Exam w/PBQ & Solution, question 5
- ? 5: What's on the CompTIA Network+ 008 certification? | CompTIA, section 3.1

NEW QUESTION 231

- (Topic 3)

An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

- A. Fiber
- B. Leased line
- C. Satellite
- D. Metro optical

Answer: C

Explanation:

If an ISP is unable to provide services to a user in a remote area through cable and DSL, the next best solution to provide services without adding external infrastructure would likely be satellite. Satellite is a wireless communication technology that uses a network of satellites orbiting the Earth to transmit and receive data. It is well-suited for providing connectivity to remote or rural areas where other types of infrastructure may not be available or may be cost-prohibitive to install.

NEW QUESTION 234

- (Topic 3)

An on-call network technician receives an automated email alert stating that a power supply on a firewall has just powered down. Which of the following protocols would best allow for this level of detailed device monitoring?

- A. TFTP
- B. TLS
- C. SSL
- D. SNMP

Answer: D

Explanation:

SNMP stands for Simple Network Management Protocol, and it is a protocol that allows network devices to communicate their status, performance, and configuration information to a central management system. SNMP can be used to monitor and manage various aspects of network devices, such as CPU usage, memory utilization, interface statistics, temperature, voltage, power supply, etc. SNMP can also generate alerts or notifications when certain events or thresholds are reached, such as a power supply failure, a link down, or a high traffic volume. SNMP is widely used for network monitoring and troubleshooting purposes, as it provides a comprehensive and detailed view of the network health and performance.

The other options are not correct because they are not protocols that allow for detailed device monitoring. They are:

? TFTP. TFTP stands for Trivial File Transfer Protocol, and it is a protocol that allows for simple and fast file transfer between network devices. TFTP is often used to transfer configuration files, firmware updates, or boot images to network devices, such as routers, switches, or firewalls. TFTP does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

? TLS. TLS stands for Transport Layer Security, and it is a protocol that provides encryption and authentication for data transmission over a network. TLS is often used to secure web traffic, email, or other applications that use TCP as the transport protocol. TLS does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

? SSL. SSL stands for Secure Sockets Layer, and it is a protocol that provides encryption and authentication for data transmission over a network. SSL is the predecessor of TLS, and it is still used to secure some web traffic, email, or other applications that use TCP as the transport protocol. SSL does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

References1: What is SNMP? - Definition from WhatIs.com2: Network+ (Plus) Certification

| CompTIA IT Certifications3: What is TFTP? - Definition from WhatIs.com4: What is TLS? - Definition from WhatIs.com5: What is SSL? - Definition from WhatIs.com

NEW QUESTION 236

- (Topic 3)

Which of the following security controls indicates unauthorized hardware modifications?

- A. Biometric authentication
- B. Media device sanitization
- C. Change management policy
- D. Tamper-evident seals

Answer: A

NEW QUESTION 238

SIMULATION - (Topic 3)

After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then

use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Network Health

Device Monitoring

Show Question

Reset All Answers

Device Status

Alert (3)

Up (8)

Warning (2)

Down (1)

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

Select Answer

Router A

Router B

WAP1

WAP2

WirelessController

Switch A

Switch B

DHCP Server

Web Server

APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer

10.1.99.28

10.1.99.14

10.1.99.10

10.1.99.22

10.1.99.24

206.208.133.10

206.208.133.9

10.1.50.14

10.1.50.13

10.1.59.81

10.1.90.53

10.1.90.55

206.208.133.9

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

? WAN 1:

? WAN 2:

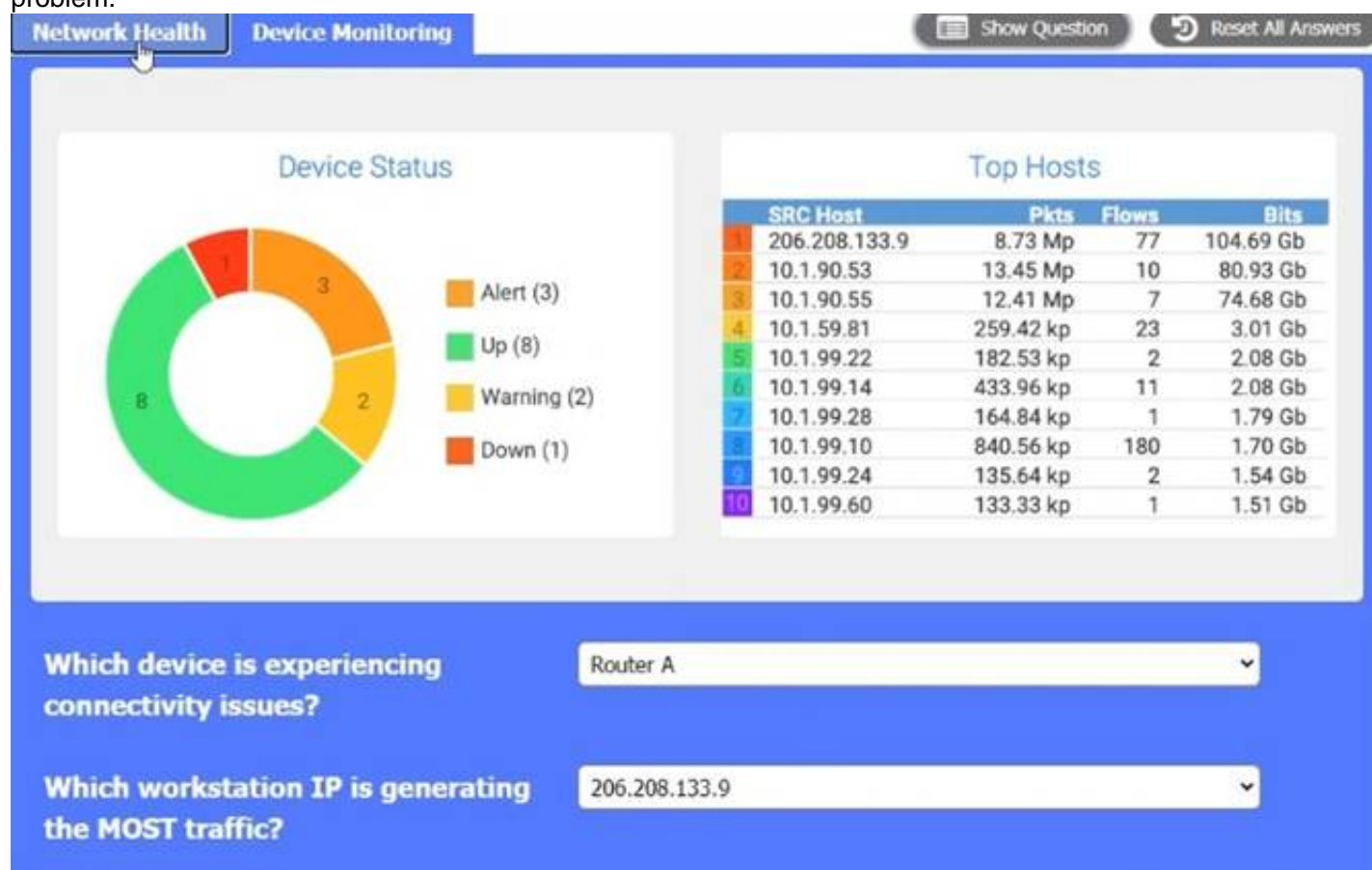
For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.



Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.



A screenshot of a computer
Description automatically generated

NEW QUESTION 239

- (Topic 3)

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

- A. Enable spanning tree.
- B. Configure port security.
- C. Change switch port speed limits.
- D. Enforce 802.1Q tagging.

Answer: A

Explanation:

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time. References:

? CompTIA Network+ N10-008 Certification Exam Objectives, page 91

? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION 241

- (Topic 3)

Which of the following is most likely to have the HIGHEST latency while being the most accessible?

- A. Satellite
- B. DSL
- C. Cable
- D. 4G

Answer: A

NEW QUESTION 245

- (Topic 3)

While using a secure conference call connection over a corporate VPN, a user moves from a cellular connection to a hotel wireless network. Although the wireless connection and the VPN show a connected status, no network connectivity is present. Which of the following is the most likely cause of this issue?

- A. MAC filtering is configured on the wireless connection.
- B. The VPN and the WLAN connection have an encryption protocol mismatch.
- C. The WLAN is using a captive portal that requires further authentication.
- D. Wireless client isolation is enforced on the WLAN settings.

Answer: C

Explanation:

A captive portal is a web page that is displayed to newly connected users of a Wi-Fi network before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of an end-user license agreement, acceptable use policy, survey completion, or other valid credentials that both the host and user agree to adhere by123

A possible cause of the issue is that the user has not completed the captive portal authentication process, which prevents the VPN from establishing a secure connection over the Wi-Fi network. The user may need to open a web browser and follow the instructions on the captive portal page to gain full access to the internet.

NEW QUESTION 246

- (Topic 3)

A company needs a redundant link to provide a channel to the management network in an incident response scenario. Which of the following remote access methods provides the BEST solution?

- A. Out-of-band access
- B. Split-tunnel connections
- C. Virtual network computing
- D. Remote desktop gateways

Answer: A

Explanation:

Out-of-band access is a remote access method that provides a separate, independent channel for accessing network devices and systems. Out-of-band access uses a dedicated network connection or a separate communication channel, such as a dial- up or cellular connection, to provide access to network devices and systems. This allows an administrator to access the management network even if the primary network connection is unavailable or impaired. Out-of-band access is a good solution for providing a redundant link to the management network in an incident response scenario because it can be used to access the network even if the primary connection is unavailable or impaired.

NEW QUESTION 249

- (Topic 3)

Which of the following can be used to identify users after an action has occurred?

- A. Access control vestibule
- B. Cameras
- C. Asset tag
- D. Motion detectors

Answer: B

Explanation:

Cameras can be used to identify users after an action has occurred by recording their faces, clothing, or other distinctive features. Cameras are often used as a deterrent and a forensic tool for security purposes. Access control vestibules, asset tags, and motion detectors are not effective in identifying users, but rather in controlling access, tracking assets, and detecting movement.

References:

CompTIA Network+ N10-008 Certification Exam Objectives, Domain 5.0: Network Security, Subobjective 5.1: Summarize the importance of physical security controls, page 231 CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008), Chapter 18: Network Security, Section: Physical Security, page 7372

NEW QUESTION 250

- (Topic 3)

A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:

- The IP address should use the highest address available in the subnet.
- The default gateway needs to be set to 172.28.85.94.
- The subnet mask needs to be 255.255.255.224.

Which of the following addresses should the engineer apply to the device?

- A. 172.28.85.93
- B. 172.28.85.95
- C. 172.28.85.254
- D. 172.28.85.255

Answer: A

Explanation:

<https://www.tunnelsup.com/subnet-calculator/>

IP Address: 172.28.85.95/27 Netmask: 255.255.255.224

Network Address: 172.28.85.64

Usable Host Range: 172.28.85.65 - 172.28.85.94

Broadcast Address: 172.28.85.95

NEW QUESTION 255

- (Topic 3)

Following the implementation of a BYOO policy, some users in a high-density environment report slowness over the wireless connection. Some wireless controller reports indicate high latency and airtime contention. Which of the following is the most probable root cause?

- A. The AP is configured with 2.4GHz frequency, which the new personal devices do not support.
- B. The AP is configured with 2.4GHz frequency without band-steering capabilities.
- C. The AP is configured with 5Ghz frequency with band-steering capabilities.
- D. The AP is configured with 5Ghz frequency
- E. which the new personal devices do not support

Answer: B

Explanation:

Band-steering is a feature that allows an AP to steer dual-band capable clients to the less congested 5GHz frequency, leaving the 2.4GHz frequency for legacy clients. Without band-steering, the AP may have more clients competing for the same channel on the 2.4GHz frequency, resulting in high latency and airtime contention.

References:

? According to the CompTIA Network+ Certification Exam Objectives, one of the topics covered in the exam is "Given a scenario, use appropriate wireless technologies and configurations". One of the subtopics is "Band steering" 1.

? According to the Polifi: Airtime Policy Enforcement for WiFi paper, "Band steering allows the access point to disable the 2.4 GHz band from probing the client device, so it responds only to the 5 GHz band, reducing the congestion on the 2.4 GHz band while taking advantage of the faster 5GHz band to improve user's network experience." 2.

? According to the Aruba Air Slice Tech Brief, "Air Slice minimizes airtime contention and efficiently groups Wi-Fi 6 and non-Wi-Fi 6 client devices to guarantee bit rate, and provide bounded latency and jitter simultaneously." 3.

NEW QUESTION 257

- (Topic 3)

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

- A. Check to see if the end connections were wrapped in copper tape before terminating.
- B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
- C. Connect the RX/TX wires to different pins.
- D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: A

Explanation:

Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable.

Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

References:

? CompTIA Network+ N10-008 Certification Study Guide, page 191

? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362

? CAT8 RJ45 Keystone Problem : r/HomeNetworking2

? How to Terminate Cat8 Shielded Keystone Jacks3

NEW QUESTION 258

- (Topic 3)

A device is connected to a managed Layer 3 network switch. The MAC address of the device is known, but the static IP address assigned to the device is not. Which of the following features of a Layer 3 network switch should be used to determine the IPv4 address of the device?

- A. MAC table
- B. Neighbor Discovery Protocol
- C. ARP table
- D. IPConfig
- E. ACL table

Answer: C

Explanation:

The ARP table is a database that is used by a device to map MAC addresses to their corresponding IP addresses. When a device sends a packet to another device on the same network, it uses the MAC address of the destination device to deliver the packet. The ARP table allows the device to determine the IP address of the destination device based on its MAC address.

NEW QUESTION 262

- (Topic 3)

Which of the following is a valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure?

- A. NFV
- B. SDWAN
- C. Networking as code
- D. VIP

Answer: A

Explanation:

The valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure is NFV (Network Function Virtualization). NFV is a technique that allows network functions, such as proxies, firewalls, routers, or load balancers, to be implemented as software applications running on virtual machines or containers. NFV reduces the need for dedicated hardware devices and improves scalability and flexibility of network services. References: CompTIA Network+ N10-008 Certification Study Guide, page 440; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-11.

NFV can be used to virtualize a wide variety of network functions, including proxy servers. By virtualizing proxy servers, organizations can save physical space in the data center and

improve the scalability and efficiency of their networks.

To virtualize a proxy server using NFV, an organization would need to deploy a virtualization platform, such as VMware ESXi or Microsoft Hyper-V. The organization would then need to install a virtual proxy server appliance on the virtualization platform.

Once the virtual proxy server appliance is installed, it can be configured and used just like a physical proxy server.

NFV is a relatively new technology, but it is quickly gaining popularity as organizations look for ways to improve the efficiency and scalability of their networks.

NEW QUESTION 263

- (Topic 3)

A network administrator received a report stating a critical vulnerability was detected on an application that is exposed to the internet. Which of the following is the appropriate NEXT step?

- A. Check for the existence of a known exploit in order to assess the risk
- B. Immediately shut down the vulnerable application server.
- C. Install a network access control agent on the server.
- D. Deploy a new server to host the application.

Answer: A

Explanation:

The appropriate next step in this situation would be to check for the existence of a known exploit in order to assess the risk. This is important because it will help the network administrator determine the severity of the vulnerability and the potential impact it could have on the organization. Once the network administrator has assessed the risk, they can then take appropriate action to address the vulnerability. This might include patching the application, deploying a new server to host the application, or implementing other security measures to mitigate the risk. It is generally not advisable to immediately shut down the vulnerable application server, as this could disrupt business operations and cause significant downtime. Similarly, installing a network access control agent on the server may not be the most effective solution, as it would not address the underlying vulnerability.

NEW QUESTION 266

- (Topic 3)

A network administrator is setting up a new phone system and needs to define the location where VoIP phones can download configuration files. Which of the following DHCP services can be used to accomplish this task?

- A. Scope options
- B. Exclusion ranges
- C. Lease time
- D. Relay

Answer: A

Explanation:

To define the location where VoIP phones can download configuration files, the network administrator can use scope options within the Dynamic Host Configuration Protocol (DHCP) service. Scope options are a set of values that can be configured within a DHCP scope, which defines a range of IP addresses that can be leased to clients on a network. One of the scope options that can be configured is the option for the location of the configuration file server, which specifies the URL or IP address of the server where the configuration files can be downloaded.

<https://pbxbook.com/voip/dhcpcfg.html>

NEW QUESTION 268

- (Topic 3)

An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

- A. Cat 7
- B. Single-mode
- C. Multimode
- D. Cat 6

Answer: B

Explanation:

Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks.

Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic

interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents.
References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]
Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.
Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.
Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth. When choosing a cable type for a long-distance application, it is important to consider the following factors:
? Attenuation: The amount of signal loss that occurs over the length of the cable.
? Bandwidth: The amount of data that can be transmitted over the cable per second.
? Cost: The cost of the cable and installation.
Single-mode fiber optic cable is the best choice for long-distance applications because it has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION 270

- (Topic 3)

A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation included air circulation, building power redundancy, and the need for continuous monitoring. The network engineer is creating alerts based on the following operation specifications:

AC input voltage	100 to 240VAC
AC maximum input current	<2.7A at 100V
Redundant power supply	Yes
Operating temperature	32–104°F (0–40°C)
Storage temperature	-4–149°F (-20–65°C)
Operating humidity	10–85%
Storage humidity	5–95%

Which of the following should the network engineer configure?

- A. Environmental monitoring alerts for humidity greater than 95%
- B. SIEM to parse syslog events for a failed power supply
- C. SNMP traps to report when the chassis temperature exceeds 95°F (35°C)
- D. UPS monitoring to report when input voltage drops below 220VAC

Answer: C

Explanation:

The alert that the network engineer should configure based on the operation specifications is SNMP traps to report when the chassis temperature exceeds 95°F (35°C). SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate their status and performance information to a central management system, called an SNMP manager. SNMP traps are messages that are sent by network devices to notify the SNMP manager of an event or condition that requires attention, such as an error, a failure, or a threshold violation. In this case, the network engineer should configure SNMP traps on the network devices to send an alert when their chassis temperature exceeds 95°F (35°C), which is the maximum operating temperature specified in the table. This alert would help the network engineer monitor and troubleshoot any overheating issues that could affect the network performance or availability. References: CompTIA Network+ N10-008 Certification Study Guide, page 228; The Official CompTIA Network+ Student Guide (Exam N10-008), page 8-11.

NEW QUESTION 273

- (Topic 3)

A network administrator is setting up a web-based application for a company. The application needs to be continually accessible to all end users. Which of the following would best ensure this need is fulfilled?

- A. NIC teaming
- B. Cold site
- C. Snapshots
- D. High availability

Answer: D

Explanation:

High availability is a quality of a system or component that assures a high level of operational performance for a given period of time. High availability means that an IT system, component, or application can operate at a high level, continuously, without intervention, for a given time period. High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime. High availability is important for web-based applications, as it ensures that the application is always accessible to the end users, even in the event of a server or component failure. High availability can be achieved by eliminating single points of failure, implementing redundancy, load balancing, and failover mechanisms.

NEW QUESTION 277

- (Topic 3)

A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

- A. B
- B. AC
- C. AX
- D. N
- E. G

Answer: B

Explanation:

Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications such as HD video streaming and online gaming. References: Network+ Study Guide Objective 2.2: Explain the purposes and properties of routing and switching. Subobjective: Wireless standards and their characteristics.

NEW QUESTION 282

- (Topic 3)

An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.

The tool was configured to scan using the following information: Network address: 172.28.16.0

CIDR: /22

The engineer collected the following information from the client workstation: IP address: 172.28.17.206

Subnet mask: 255.255.252.0

Which of the following MOST likely explains why the tool is failing to detect some workstations?

- A. The scanned network range is incorrect.
- B. The subnet mask on the client is misconfigured.
- C. The workstation has a firewall enabled.
- D. The tool is unable to scan remote networks.

Answer: C

Explanation:

A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.

References: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

NEW QUESTION 286

- (Topic 3)

A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

- A. Asymmetric routing
- B. A routing loop
- C. A switch loop
- D. An incorrect gateway

Answer: C

NEW QUESTION 290

- (Topic 3)

An organization would like to implement a disaster recovery strategy that does not require a facility agreement or idle hardware. Which of the following strategies MOST likely meets the organization's requirements?

- A. Cloud site
- B. Cold site
- C. Warm site
- D. Hot site

Answer: A

Explanation:

A cloud site is a type of disaster recovery site that uses cloud computing services to provide backup and recovery of data and applications in the event of a disaster¹. A cloud site does not require a facility agreement or idle hardware, as the cloud provider manages the infrastructure and resources on demand. A cloud site can also offer scalability, flexibility, and cost-effectiveness compared to other types of disaster recovery sites.

NEW QUESTION 294

- (Topic 3)

A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

- A. Adding more wireless APS
- B. Increasing power settings to expand coverage
- C. Configuring the APS to be compatible with 802.11a
- D. Changing the wireless channel used

Answer: C

Explanation:

* 802.11g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.

References: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

NEW QUESTION 299

- (Topic 3)

An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, the administrator sees the following entries:

Rule	Action	Source	Destination	Port
1	Deny	Any	172.30.10.50	Any
2	Deny	Any	232.1.4.9	Any
3	Deny	Any	242.9.15.4	Any
4	Deny	Any	175.50.10.10	Any

Which of the following firewall rules is MOST likely causing the issue?

- A. Rule 1
- B. Rule 2
- C. Rule 3
- D. Rule 4

Answer: A

NEW QUESTION 300

- (Topic 3)

Which of the following would be the BEST choice to connect branch sites to a main office securely?

- A. VPN headend
- B. Proxy server
- C. Bridge
- D. Load balancer

Answer: A

Explanation:

Host-to-Site, or Client-to-Site, VPN allows for remote servers, clients, and other hosts to establish tunnels through a VPN gateway (or VPN headend) via a private network. The tunnel between the headend and the client host encapsulates and encrypts data.

NEW QUESTION 305

- (Topic 3)

A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified in the SLA.

Which of the following would BEST help measure the throughput?

- A. iPerf
- B. Ping
- C. NetFlow
- D. Netstat

Answer: A

NEW QUESTION 306

- (Topic 3)

A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

- A. Coaxial over Ethernet
- B. Internet Small Computer Systems Interface
- C. Fibre Channel
- D. Gigabit interface converter

Answer: C

Explanation:

The transceivers labeled 8Gbps are likely to be used with the Fibre Channel protocol. Fibre Channel is a high-speed networking technology that is primarily used to connect storage devices to servers in storage area networks (SANs). It is capable of transmitting data at speeds of up to 8 Gbps (gigabits per second), and uses specialized transceivers to transmit and receive data over fiber optic cables.

Coaxial over Ethernet (CoE) is a networking technology that uses coaxial cables to transmit data, and is not related to the transceivers in question. Internet Small Computer Systems Interface (iSCSI) is a protocol that allows devices to communicate over a network using the SCSI protocol, and does not typically use specialized transceivers. Gigabit interface converter (GBIC) is a type of transceiver used to transmit and receive data over fiber optic cables, but it is not capable of transmitting data at 8 Gbps.

NEW QUESTION 308

- (Topic 3)

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a recurrence. Which of the following should the firewall administrator do next?

- A. Consult the firewall audit logs.
- B. Change the policy to allow port 80.
- C. Remove the server object from the firewall policy.
- D. Check the network baseline.

Answer: A

Explanation:

Firewall audit logs are records of the changes made to the firewall configuration, policies, and rules. They can help the firewall administrator to track who, when, and what changes were made to the firewall, and identify any unauthorized or erroneous modifications that could cause security issues or network outages. By consulting the firewall audit logs, the firewall administrator can investigate how the change that allowed traffic on port 80 to the web server occurred, and prevent it from happening again

NEW QUESTION 313

- (Topic 3)

A network technician is troubleshooting a connectivity issue. All users within the network report that they are unable to navigate to websites on the internet; however, they can still access local network resources. The technician issues a command and receives the following results:

```
Pinging comptia.com [172.67.217.56] with 32 bytes of data:
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
```

Which of the following best explains the result of this command?

- A. Incorrect VLAN settings
- B. Upstream routing loop
- C. Network collisions
- D. DNS misconfiguration

Answer: D

Explanation:

The users are unable to navigate to websites on the internet but can access local network resources, indicating a possible DNS issue. The ping command result showing “TTL expired in transit” suggests that packets are not reaching their destination due to a DNS misconfiguration that is not resolving website names into IP addresses correctly³. A possible solution is to check and correct the DNS server settings on the network devices⁴.

References: 3: What does “TTL expired in transit” mean?⁵4: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring²

NEW QUESTION 315

- (Topic 3)

A network technician is having issues connecting an IoT sensor to the internet The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless interlace. However, when trying to connect to the internet, only HTTP redirections are being received when data is requested. Which of the following will point to the root cause of the Issue?

- A. Verifying if an encryption protocol mismatch exists.
- B. Verifying If a captive portal is active for the WLAN.
- C. Verifying the minimum RSSI for operation in the device's documentation
- D. Verifying EIRP power settings on the access point.

Answer: C

Explanation:

A captive portal is a web page that is displayed to a user before they can access the internet or other network resources. This is often used in public or guest networks to present users with a login or terms and conditions page before they can access the internet. If a captive portal is active on the WLAN, it would explain why the IoT sensor is only receiving HTTP redirections when trying to connect to the internet.

NEW QUESTION 316

- (Topic 3)

Which of the following DHCP settings would be used to ensure a device gets the same IP address each time it is connected to the network?

- A. Scope options
- B. Reservation
- C. Exclusion
- D. Relay
- E. Pool

Answer: A

NEW QUESTION 320

- (Topic 3)

A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

- A. Incorrect VLAN setting
- B. Insufficient DHCP scope
- C. Improper NIC setting
- D. Duplicate IP address

Answer: B

NEW QUESTION 321

- (Topic 3)

To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

- A. Public
- B. Hybrid
- C. SaaS
- D. Private

Answer: B

Explanation:

A hybrid cloud deployment model is a combination of on-premise and cloud solutions, where some resources are hosted in-house and some are hosted by a cloud provider. A hybrid cloud model can offer the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control¹². A hybrid cloud model can also reduce the impact for users, as they can access the key services from the on-site data center and the enterprise services from the cloud

NEW QUESTION 324

- (Topic 3)

A user took a laptop on a trip and made changes to the network parameters while at the airport. The user can access all internet websites but not corporate intranet websites. Which of the following is the most likely cause of the issue?

- A. Duplicate IP address
- B. Duplicate SSID
- C. Incorrect DNS
- D. Incorrect subnet mask

Answer: C

Explanation:

DNS (Domain Name System) is a service that translates domain names into IP addresses. Corporate intranet websites are usually hosted on private IP addresses that are not accessible from the public internet. Therefore, the user's laptop needs to use the correct DNS server that can resolve the intranet domain names to the private IP addresses. If the user changed the network parameters at the airport and did not revert them back, the laptop might be using a public DNS server that does not have the records for the intranet websites. This would cause the user to access all internet websites but not corporate intranet websites.

References:

? An Overview of DNS - N10-008 CompTIA Network+ : 1.61

? DNS Configuration – CompTIA A+ 220-11012

? CompTIA Network+ Certification Exam Objectives, page 53

NEW QUESTION 329

- (Topic 3)

Which of the following issues are present with RIPv2? (Select TWO).

- A. Route poisoning
- B. Time to converge
- C. Scalability
- D. Unicast
- E. Adjacent neighbors
- F. Maximum transmission unit

Answer: BC

Explanation:

The disadvantages of RIP (Routing Information Protocol) include the following.

---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.

---The more well-known problem of the 15 hop limitation in which data must travel

---Convergence time is terrible for information propagation in a network

---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel

---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'.
RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION 331

- (Topic 3)

Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of the following actions can reduce repair time?

- A. Using a tone generator and wire map to determine the fault location
- B. Using a multimeter to locate the fault point
- C. Using an OTDR In one end of the optic cable to get the fiber length information
- D. Using a spectrum analyzer and comparing the current wavelength with a working baseline

Answer: C

NEW QUESTION 332

- (Topic 3)

Which of the following network cables involves bouncing light off of protective cladding?

- A. Twinaxial
- B. Coaxial
- C. Single-mode
- D. Multimode

Answer: D

Explanation:

Multimode fiber optic cables use multiple paths of light that bounce off the cladding, which is a layer of glass or plastic that surrounds the core of the cable.
<https://www.explainthatstuff.com/fiberoptics.html>

NEW QUESTION 333

- (Topic 3)

Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

- A. Fiber distribution panel
- B. 110 punchdown block
- C. PDU
- D. TIA/EIA-568A patch bay
- E. Cat 6 patch panel

Answer: A

Explanation:

A fiber distribution panel is a device that provides a central location for connecting and managing fiber optic cables and optical modules. It can support various types and speeds of fiber optic links, including multimode uplinks. Therefore, a fiber distribution panel should be used to manage outside cables that need to be routed to various multimode uplinks.

NEW QUESTION 338

- (Topic 3)

Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

- A. Site survey
- B. EIRP
- C. AP placement
- D. Captive portal
- E. SSID assignment
- F. AP association time

Answer: AC

Explanation:

This is a coverage issue. WAP placement and power need to be checked. Site survey should be done NEXT because it takes a while.

NEW QUESTION 342

- (Topic 3)

A company's web server is hosted at a local ISP. This is an example of:

- A. allocation.
- B. an on-premises data center.
- C. a branch office.
- D. a cloud provider.

Answer: D

NEW QUESTION 343

- (Topic 3)

Which of the following would MOST likely be used to review disaster recovery information for a system?

- A. Business continuity plan
- B. System life cycle
- C. Change management
- D. Standard operating procedures

Answer: A

Explanation:

The document that would most likely be used to review disaster recovery information for a system is a business continuity plan (BCP). A BCP is a document that outlines the procedures and resources needed to maintain or resume critical business functions in the event of a disaster or disruption. A BCP typically includes a disaster recovery plan (DRP), which is a subset of the BCP that focuses on restoring IT systems and data after a disaster. A BCP also covers other aspects of business continuity, such as risk assessment, business impact analysis, emergency response, crisis management, and testing. References: CompTIA Network+ N10-008 Certification Study Guide, page 346; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-9.

NEW QUESTION 345

- (Topic 3)

A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

- A. Coaxial over Ethernet
- B. Internet Small Computer Systems Interface
- C. Fibre Channel
- D. Gigabit interface converter

Answer: C

Explanation:

Fibre Channel is a high-speed network technology that is mainly used for storage area networks (SANs). It provides reliable and secure data transfer between servers and storage devices, such as disk arrays, tape libraries, and optical jukeboxes. It uses protocols such as SCSI, FCP, and FICON to transport data over optical fiber or copper cables. Fibre Channel transceivers are devices that convert electrical signals to optical signals and vice versa, and allow Fibre Channel devices to communicate over different media types

and distances. They are usually pluggable modules that fit into standard ports on Fibre Channel switches, adapters, and storage devices. They have different specifications and standards, such as SFP, SFP+, QSFP, and CFP, depending on the data rate, wavelength, and cable type they support.

8 Gbps transceivers are Fibre Channel transceivers that support a data rate of 8 gigabits per second, which is also known as Fibre Channel-8G or 8GFC. They are typically SFP+ modules that use 850 nm wavelength and multimode fiber for short-reach applications, or 1310 nm wavelength and single-mode fiber for long-reach applications. They can support cable distances up to 10 km or 40 km, depending on the fiber type and quality.

NEW QUESTION 348

- (Topic 3)

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

- A. Replace the Cat 5 patch cable with a Cat 6 cable
- B. Install a crossover cable between the server and the switch
- C. Reset the switchport configuration.
- D. Use NetFlow data from the switch to isolate the issue.
- E. Disable MDIX on the switchport and reboot the server.

Answer: A

Explanation:

"Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted."

NEW QUESTION 350

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your N10-008 Exam with Our Prep Materials Via below:

<https://www.certleader.com/N10-008-dumps.html>